Release Notes: Windows Sensor v6.2.4

September 2019

Summary

Cb Response Windows Sensor v6.2.4 is intended to provide Network Isolation Exclusions, Tamper Hardening, performance improvements, stability improvements and bug fixes. This sensor release also includes all changes and fixes from previous releases.

This document provides information for users upgrading to Cb Response Windows Sensor v6.2.4 from previous versions as well as users new to Cb Response. The key information specific to this release is provided in the following major sections:

- **Installation Instructions** - Provides instructions for Windows Response sensor installation.
- **New features** – Describes new features introduced in this release.
- **Corrective content** – Describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known issues and limitations** – Describes known issues or anomalies in this version that you should be aware of.

Server compatibility

Cb Response sensors included with Cb Response server releases are compatible with all server releases going forward. It is always recommended to use the latest server release with our latest sensors to utilize the full feature capabilities of our product, however, using earlier 6.x server versions with the latest sensor should not impact core product functionality.

Sensor operating systems

Cb Response sensors interoperate with multiple operating systems. For the most up-to-date list of supported operating systems for Cb Response sensors (and all Carbon Black products), refer to the following location in the Carbon Black User eXchange:
https://community.carbonblack.com/docs/DOC-7991

Documentation

This document supplements other Carbon Black documentation. Click here to search the full library of Cb Response user documentation on the Carbon Black User eXchange.

Technical support

Cb Response server and sensor update releases are covered under the Customer Maintenance Agreement. Technical Support is available to assist with any issues that might develop during the installation or upgrade process. Our Professional Services organization is also available to assist to ensure a smooth and efficient upgrade or installation.

Note: Before performing an upgrade, Carbon Black recommends reviewing content on the User eXchange for the latest information that supplements the information contained in this document.

Installation Instructions

To install the sensors on to your server, run through the following instructions:

1. Ensure your CB Response YUM repo is set appropriately:
    a. The CB Response repository file to modify is */etc/yum.repos.d/CarbonBlack.repo*
    b. Baseurl = https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/
2. On the CB Response server, clear the YUM cache by running the following command:
    a. *yum clean all*
3. After the YUM cache has been cleared, download the sensor install package by running the following command:
    a. Run *yum install --downloadonly --downloaddir=<package local download directory> <package>*
        i. **Note:** The *<package local download directory>* is a directory of your choice
        ii. **Note:** *<package>* is replaced by *cb-sensor-6.2.4.90820-win*
4. Install the new sensor package on the CB Response server by running the command:
    a. *rpm -i --force <package>*
5. Make the new installation package available in the server console UI by running the command:
    a. */usr/share/cb/cbcheck sensor-builds --update*
        i. **Note:** If your groups have *Automatic Update* enabled, the sensors in that group will start to automatically update.

Your new sensor versions should now be available via the console. For any issues, please contact Carbon Black Technical Support.

New Features

- **Tamper Hardening Improvements** - The v6.2.4 Windows sensor more thoroughly authenticates communications between our cb.exe service and drivers to mitigate possible malicious exploits. [CB-26624]
- **Network Isolation Exclusions** - In conjunction with the CB Response Server 6.5.0, this feature allows CB Response users to add a set of IP addresses or URLs to exclude from network isolation on a per sensor group basis. Threat Hunters & Incident Responders can allow IT tools, VPN and proxy connections, and other security tools to continue to operate while putting the sensor in isolation. [CB-27390]

Corrective Content

This release provides the following corrective content changes:

- Fixed an issue with attempting to rename sensor binary/service name in the event renaming initially fails. [CB-22642]
- Improved driver logging. [CB-24406]
- Fixed an issue with Isolation during periods of idle time. [CB-24725]
- Datastore.log file is now captured for dumping diagnostic files to disk. [CB-25681]
- Fixed an issue where sensor unnecessarily calculated hashes for some processes. [CB-25828]
- Fixed an issue where generating memory dumps using Live Response could cause bugchecks if “VBS” setting was enabled. [CB-26013]
- Fixed an issue with upgrading uninst.exe during sensor upgrades. [CB-26034]
- Updated sensor to not download certificate revocation lists when verifying code signatures. [CB-26427]
- Updated sensor to inspect basic constraint certificate details when sensor is in “strict cert” mode. [CB-26621]
- Updated sensor to preserve hashes calculated for process events observed (but not collected) to improve sensor performance on heavily used systems. [CB-27008]
- Updated sensor to preserve hashes calculated for binaries observed (but not collected) to improve sensor performance on heavily used systems. [CB-27009]
- Fixed an issue where Live Response sessions were capped at a throttle limit of 512 Kb/s. [CB-27027]
- Fixed an issue where eventlog upload queue could significantly backup if a large number of store files for upload is observed. [CB-27029]

- Fixed an issue where exceeding set number of worker threads on Windows7/Server2012 R2 could cause a deadlock to the NTFS driver of the host. [CB-27151]
- Increased file read chunk size to improve sensor performance on heavily used systems. [CB-27320]
- Fixed an issue where legacy registry information relating to the Windows Response sensor remained after upgrades to latest Windows Response sensor. [CB-27616]
- Updated sensor to reject sensor-server communications if certificate revocation status is revoked when sensor is in “strict cert” mode. [CB-27766]
- Fixed an issue where Tamper Detection events could fail to send to server on Windows 7 endpoints. [CB-28037]
- Fixed an issue where Tamper Detection events could fail to send to server on Windows Server 2012 R2 endpoints. [CB-28039]
- Fixed an issue where restarting the sensor through the server with Tamper Detection enabled could result in a reduced health score. [CB-28087]
- Addressed an issue that causes cb.exe to encounter an insufficient resources error. [CB-21837]

Known Issues and Limitations

Known issues associated with this version of the sensor are included below:

- **Disabling DNS Name Resolution For NetConn Events:** Customers have observed that the Windows sensor can report high CPU utilization by the Carbon Black service (‘cb.exe’) on machines with a continually large number of network connections (e.g. DHCP/DNS servers, Domain Controllers, etc.). To help alleviate the high CPU utilization, without having to disable collection of network connection events, the windows sensor can be configured to disable DNS name resolution in data collection for network connection events by configuring the windows registry key [CB-17552]:

  [HKEY_LOCAL_MACHINE\SOFTWARE\CarbonBlack\config]

  "DisableNetConnNameResolution"=dword:00000001

- **Tamper Detection Events Generated When Restarting Sensor Service from Response Server:** Customers restarting the sensor service from the Response server console, with Tamper Detection enabled, will observe Tamper Detection alerts that will be assigned to the cb.exe process of the outgoing process. [CB-21882]

- **Netconn Events Not Reported for URLs Excluded From Isolation:** URLs that are designated as a Network Isolation Exclusion may fail to report the associated Netconn event under the Process Search page when the sensor is in Isolation mode. [CB-28100]

- **Obfuscated Windows Sensors Will Not Start After First Reboot:** Windows sensors installed from an obfuscated sensor group will not start after first reboot. A second reboot will start the sensor service. [CB-28062]
- **CB Entries Remaining in Add/Remove Programs:** Customers uninstalling their Cb Response Windows sensor through uninst.exe will notice remaining Cb entries in the Add/Remove Programs window. [CB-28059]
- **CB Branding Is Different Between MSI and EXE Installers:** Customers using the Add/Remove Program window to manage their Cb Response installation should be aware that the CB branding between the MSI and EXE installers is different. [CB-28063]
- **Install/Uninstall & Upgrade/Downgrade of Sensor on WinXP & WinServer2003 Requires Reboot:** Customers running the Windows sensor on a Windows XP or Windows Server 2003 machine should note that a reboot of the machine will be required for all install/uninstall and upgrade/downgrade methods in order to successfully load and unload Cb drivers. [CB-28261]
- **CB Protection Upgrade Needed:** Customers who are running Cb Protection to tamper protect the Cb Response Sensor and do not opt-in to CDC will need to update their tamper rule settings for Cb Protection to the latest “Cb Response Tamper Protection” Rapid Config (if running CbP 8.x) or Updater (if running CbP 7.x) in order to successfully upgrade/downgrade their Cb Response sensor. Please contact technical support to obtain the latest Rapid Config or Updater for CbP. [CB-15941]

Contacting Support

Use one of the following channels to request support or ask support questions:

- **Web:** User eXchange
- **Email:** support@carbonblack.com
- **Phone:** 877.248.9098
- **Fax:** 617.393.7499

Reporting Problems

When contacting Carbon Black Technical Support, be sure to provide the following required information about your question or issue:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (Cb Response server and sensor version)
- **Hardware configuration:** Hardware configuration of the Cb Response server (processor, memory, and RAM)
- **Document version:** For documentation issues, specify the version and/or date of the manual or document you are using
- **Problem:** Action causing the problem, error message returned, and event log output (as appropriate)

- **Problem severity:** Critical, serious, minor, or enhancement request